AMENDMENTS TO THE CLAIMS

1. (Currently amended) An apparatus, comprising:

an authentication device that authenticates a computing device, in communication with the authentication device, through employment of a determination that a current location of the authentication device matches an initial location of the authentication device;

wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device.

2. (Previously presented) The apparatus of claim 1, wherein the computing device comprises a first computing device; and

wherein the authentication device makes the determination that the current location of the authentication device matches the initial location of the authentication device in response to a request from a second computing device for authentication of the first computing device for a data transfer from the second computing device to the first computing device.

3. (Previously presented) The apparatus of claim 2, wherein the request from the second computing device comprises an authentication challenge string; and

wherein the authentication device stores the one or more private keys, and wherein if the current location of the authentication device matches the initial location of the authentication device, then the authentication device employs one or more of the one or more private keys to decrypt the authentication challenge string into an authentication challenge response.

4. (Previously presented) The apparatus of claim 3, wherein the authentication device sends the authentication challenge response to the second computing device, and wherein the second computing device analyzes the authentication challenge response to determine whether the first computing device is authenticated for the data transfer.

5. (Previously presented) The apparatus of claim 4, wherein the second computing device comprises an authentication challenge key to compare with the authentication challenge response received from the authentication device; and

wherein if the authentication challenge response matches the authentication challenge key, then the authentication challenge response represents that the first computing device is authenticated and the data transfer can be sent from the second computing device to the first computing device.

6. (Original) The apparatus of claim 3, wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device prevents authentication of the first computing device and disables the one or more private keys.

7. (Previously presented) The apparatus of claim 6, wherein the authentication device stores the one or more private keys in volatile memory, and wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device cuts off power to the volatile memory to erase the one or more private keys.

8. (Previously presented) The apparatus of claim 1, wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that serve to authenticate the computing device; and

wherein the base portion is fixed to a surface near the computing device, and wherein the cover portion is fixed to the base portion to provide a secure shell for the one or more electronic components.

9. (Previously presented) The apparatus of claim 8, wherein a first one of the base and cover portions receives electricity through a power port, and wherein a second one of the base and cover portions receives electricity through an electrical contact with the first one of the base and cover portions; and

wherein upon separation of the second one of the base and cover portions from the first one of the base and cover portions, the second one of the base and cover portions loses power and prevents authentication of the computing device.

10. (Previously presented) The apparatus of claim 9, wherein the second one of the base and cover portions electrically supports one or more of the one or more electronic components that store the one or more private keys, and wherein the authentication device employs one or more of the one or more private keys to authenticate the computing device; and

wherein a loss of power in the second one of the base and cover portions erases the one or more private keys from the one or more of the one or more electronic components.

11. (Previously presented) The apparatus of claim 1, wherein the authentication device comprises a location sensor; and

wherein upon initialization of the authentication device, the location sensor sets the initial location of the authentication device; and

wherein the location sensor determines the current location of the authentication device, and wherein the authentication device compares the current location with the initial location to authenticate the computing device.

12. (Previously presented) The apparatus of claim 11, wherein the location sensor comprises a global positioning system component, and wherein the global positioning system component measures the initial location and the current location of the authentication device as a three-dimensional location of latitude, longitude, and altitude.

13. (Original) The apparatus of claim 1, wherein the authentication device allows authentication of the computing device upon the determination that the current location of the authentication device matches the initial location of the authentication device within a specified error range.